A Thematic Content Analysis of the Cybersecurity Skills Demand in South Africa

Madri Kruger(✉), Lynn Futcher, and Kerry-Lynn Thomson

Nelson Mandela University, Port Elizabeth, South Africa
{madri.kruger,lynn.futcher,kerry-lynn.thomson}@mandela.ac.za

Abstract. The cybersecurity skills demand is a growing concern both globally and in South Africa, creating what is known as the cybersecurity skills gap. This means that there is a shortage of Information Technology (IT) and cybersecurity professionals that have the required knowledge, skills and abilities, to effectively fill this gap. This study aims to provide a better understanding of the cybersecurity skills demand in South Africa having analysed job postings in South Africa over a 4-month period from 1st October 2020 to 31st January 2021. This was done by conducting a thematic content analysis of the 280 job postings identified during this period. Results indicate a condensed set of knowledge, skills and abilities (KSAs) categorised according to five main job categories, namely: Cybersecurity, Operations and Support, Data and Artificial Intelligence, Strategy and Governance, and Software and Application Development. These results can assist universities, training institutions and organisations to address the cybersecurity skills gap in South Africa.

Keywords: Cybersecurity · Skills demand · Thematic content analysis

1 Introduction

The global Cyber Exposure Index ranks South Africa sixth on the list of most-targeted countries for cyberattacks [1]. According to the Kaspersky laboratory, malware attacks in South Africa increased by 22% in the first quarter of 2019 compared to the same time in 2018. This equates to about 13842 attempted cyberattacks daily, or just over 9 attacks per second [2]. Due to this growth in cyberattacks in South Africa, cybersecurity needs to grow in response in order to mitigate such attacks.

Cybersecurity is seen as the practice of defending systems, networks and programs from cyberattacks [3]. There are many threats to cybersecurity, such as phishing, malware, trojans, ransomware, worms and Denial of Service attacks (DoS), among others [4]. In addition, the personal information stored on devices like computers and mobile phones can be used for identity theft, financial gain, blackmail and for gaining access to highly confidential information.

Published by Springer Nature Switzerland AG 2022
N. Clarke and S. Furnell (Eds.): HAISA 2022, IFIP AICT 658, pp. 24–38, 2022.
https://doi.org/10.1007/978-3-031-12172-2_3

Human error is the main cause of 95% of cybersecurity breaches [5]. Through advances in the technological tools used in information and network security, a large majority of threat detection and monitoring has been automated, However, some tasks cannot be automated and require human intervention to successfully secure information and networks [6].

In a global survey by Oltsik, 82% of respondents reported a shortage of cybersecurity skills, and 61% of companies believed that cybersecurity-related job applicants are not qualified for the job [7]. In a follow-up survey in 2020, 45% of the respondents believed that the skills shortage, as well as its impact, has gotten worse over the last few years [8].

The aim of this paper is to provide a better understanding of the cybersecurity skills demand in South Africa, by analysing job postings in South Africa over a 4-month period from 1st October 2020 to 31st January 2021. This was done by conducting a thematic content analysis of 280 relevant job postings identified during this period.

This paper is structured as follows. Section 2 provides related literature regarding the cybersecurity skills gap both globally and in South Africa. In addition, it highlights several skills frameworks that provide insight into various cybersecurity work roles and their related knowledge, skills and abilities (KSAs). Section 3 discusses the thematic content analysis conducted as a key research method of this study, and Sect. 4 presents the results and findings from the thematic content analysis. Section 5 provides a discussion before concluding the paper in Sect. 6.

2 Related Literature

In 2019, ISACA conducted a survey to better understand the current state of cybersecurity globally. 58% of their respondents indicated that they have unfilled cybersecurity positions within their organisations. The study also indicated an annual 6% increase in the waiting time of positions being filled, sometimes taking as long as six months to fill such positions. Technically skilled cybersecurity professionals were considered the hardest to find, further contributing to the struggle of filling open cybersecurity positions [9].

According to Burning Glass Technologies, job postings for cybersecurity openings have grown three times as fast as openings for IT jobs overall [10]. Although some IT jobs can be filled easily without the need for extensive training, most cybersecurity jobs require specific KSAs, some of which can only be gained through specialised training.

There are many accredited certifications that a cybersecurity professional can attain, including: Certified Information Systems Security Professional (CISSP), CompTIA Security+ and Certified Ethical Hacker (CEH), to name just a few. Each certification targets a different need within industry and most of them are globally recognised. When taking into consideration that in order to apply for CISSP certification, applicants require at least 5 years of relevant experience, one can understand why there is such a huge need for skilled and trained cybersecurity employees [9]. Due to the high qualification and experience requirements for most cybersecurity-related jobs, the cybersecurity skills gap will not be easily addressed in the near future.

South Africa has also been affected by the worldwide shortage of cybersecurity skills. One of South Africa's largest banks, Absa, has collaborated with the Maharishi

Institute (MI) to set up the Absa Cybersecurity Academy in an attempt to address its skills shortage [11]. Despite these kinds of targeted efforts, there is a lack of cost-effective local cybersecurity training offered to South Africans. Most cybersecurity courses offered by international organisations are often unaffordable for most South Africans due to them being billed in US dollars [12]. This has resulted in several local universities, colleges and training institutions providing various forms of cybersecurity training and education. However, most of these would have been based on insight gained from international cybersecurity skills frameworks. For example, the National Initiative for Cybersecurity Education (NICE) framework developed by the National Institute of Standards and Technology (NIST), a United States based institute.

The NICE framework attempts to create a better understanding of what cybersecurity jobs entail and what knowledge, skills, and abilities (KSAs) are needed to complete certain tasks based on job roles. This is a useful tool for organisations seeking guidance on their cybersecurity workforce development. However, while the NICE framework is good at defining job descriptions, there are over 1600 KSA's and more than 50 job roles, making it rather unmanageable. In addition, some of their KSAs are vague and not well defined [13].

A further framework of particular interest to this study is the Skills Framework for Infocomm Technology (SFw for ICT). This framework aims to provide information on career paths, existing and emerging skills, as well as occupations and job roles and their respective knowledge, skills, abilities and tasks (KSATs). It is therefore useful for employers and educational facilities, as well as individuals who are job seeking or planning their careers. Although this framework does not focus specifically on cybersecurity, it does include cybersecurity as one of the seven career pathway tracks [14].

A study by Parker and Brown provides some insight into various cybersecurity jobs advertised in South Africa, together with the typical skills required by such cybersecurity professionals. However, Parker and Brown consider their work as an initial exploratory study providing a basis for future studies [6]. Further, it can be argued that cybersecurity skills are required by IT professionals at all levels of the profession since they are all personally responsible for the information they are entrusted with.

3 Thematic Content Analysis Using ATLAS.ti

Before starting the formal data collection process, it was decided to conduct a pilot study to gain a better understanding of the data to be collected for this study. In September 2020, the pilot study began. Data was collected weekly on three job posting websites, namely: LinkedIn, Careers24 and Career Junction. During the pilot study it was found that the adverts on LinkedIn provided greater depth of information compared to other job posting websites, and was therefore chosen for the rest of the study.

The official data collection for this study took place over a four-month period from 1st October 2020 to 31st January 2021. The search results were filtered by relevant IT and cybersecurity-related jobs each week and set to South African based job postings only. A total of 280 job postings were collected. These job postings were then analysed by conducting a thematic content analysis using ATLAS.ti, a popular software analysis tool for analysing qualitative data.

A three-phased approach was used for the thematic content analysis as proposed by [15]. Using ATLAS.ti in combination with this three-phased approach is considered a promising strategy for conducting a thematic content analysis [15]. Figure 1 presents the three phases of the thematic content analysis and the associated steps taken in ATLAS.ti.

Phases of thematic content analysis	Steps in ATLAS.ti
First phase: Pre-analysis.	Creating the project. Adding documents. Grouping documents into document groups. Writing first memos on the overall project aim including research questions.
Second phase: Material exploration.	Reading the data, selecting data segments and creating quotations. Creating and applying codes. Writing memos and comments. Grouping codes and memos
Third phase: Interpretation.	Exploring the coded data using various analysis tools. Linking quotations, codes, and memos on the conceptual level. Continuing memo writing. Generating network views. Extracting reports.

Fig. 1. Three-phased thematic content analysis [15]

These phases are discussed in more detail in the following sub-sections.

3.1 First Phase: Pre-analysis

Firstly, a new project was created in ATLAS.ti. All the data collected for the four months from 1st October 2020 to 31st January 2021 were added to this project by importing the MS Word documents containing the job postings for each month into the project. Once imported, these documents were grouped according to month, resulting in four groups named "OCT", "NOV", "DEC" and "JAN". Each monthly group contained four MS Word documents, one for each week of the month.

3.2 Second Phase: Material Exploration

To start the second phase of the thematic content analysis, a document group was opened, and a document was chosen. This started with the document group called "OCT", and the document for the first week of October was selected. This document was then read, and important data segments were selected, and quotations created for these segments. Each of the quotations were assigned a code. Thereafter the next document in the group was selected which in this case was called "Week 2 Oct" after it had been completed the same process was followed for the documents "Week 3 Oct" and "Week 4 Oct". Once document group "OCT" was completed, the next group was selected, that being document group "NOV", and the documents for each week in document group "NOV" completed. The same process was followed for document groups "DEC" and "JAN",

as well as their respective documents. There was a total of 640 codes and 3580 quotations after completing the coding for each of the document groups. Each quotation was linked to only one data segment. Each quotation was assigned a single code, and a code belonged to only one code group. For example, the quotation "Ideal candidate must have a Security+ certification" would be assigned the code "Security+".

Once all job postings had been coded, these codes needed to be organised. To do this, a similar process to that used for the document groups was followed, called code groups. Each of the different types of codes were grouped according to their type. For example, all certifications were grouped into a group called Certifications. The same was done for all the other types of codes. A total of six code groups were identified, namely: Certifications, Industries, Job Levels, Job Roles, Job Types and Regions.

Once all codes had been grouped, each group was inspected individually to find possible duplications. For example, in the case of the Certifications group, it contained multiple occurrences of the same certifications due to them often being referred to in various ways by different employers. One such case was the certification Security+. It was referred to as S+ in some cases and as Security+ in others. In this case the two codes were merged into a single code, named Security+.

After the codes had been grouped and checked for duplicates, there was a total of 552 codes in the project, thus a reduction of 88 from the original 640 codes.

3.3 Third Phase: Interpretation

In the third phase, the primary focus was on the code group called "Job Roles" since these could be further analysed according to their related knowledge, skills and abilities (KSAs). A total of 223 job roles were identified in the "Job Roles" code group on starting this third phase of the thematic content analysis. However, on further analysis, some of these job roles were found to be similar, but were named differently due to employers using different naming conventions. For example, a job role named "Software Developer" and a job role named "Application Developer" were merged into a single job role named "Software Developer" since they were considered to be similar job roles.

Each job role was individually assessed according to their associated knowledge, skills and abilities (KSAs) and their required certifications were noted in a comment associated with the job role. To further determine whether job roles were the same, their KSAs were compared. If they had the same KSAs, the job roles were deemed similar and were merged into one. After the completion of this phase, the initial 223 job roles were substantially reduced to a total of 20 job roles, each having defined KSAs, as well as various certifications associated with them.

The completed thematic content analysis process resulted in 353 codes spread over five key job categories, down from the initial number of 640 codes at the beginning of the Material Exploration Phase.

4 General Results and Findings

Of the 280 postings analysed, approximately 90% were full-time positions. From the thematic content analysis conducted, the following key categories were deemed most

relevant to this study, and were therefore defined and coded for further analysis. These key categories were derived from the code groups described in Sect. 3.2 and included:

- the industry (where five main industries were identified)
- the job location (this was indicated by province)
- the job level (ranging from entry-level to executive-level)
- the minimum qualifications and certifications.

These key categories are further analysed in their respective sub-sections below, while job roles and their related KSAs are discussed in Sect. 5.

4.1 Identified Industries

From the thematic content analysis conducted, it was found that most of the job postings indicated the specific industry of the job advertised. In total, there were 43 industries identified from the 280 job postings analysed. Of the identified industries Information Technology and Services was mentioned 140 times (25%), Financial Services was mentioned 122 times (21.7%) and Computer Software mentioned 84 times (15%).

4.2 Job Locations

South Africa has a total of nine provinces, eight of which had job listings during the four-month data collection period from 1st October 2020 to 31st January 2021. Gauteng accounted for most of the job postings (178 postings, 63.6%), followed by the Western Cape (67 postings, 23.9%). These two provinces, accounted for 87.5% of the total job postings.

4.3 Job Levels

Most job postings collected over the four-month period had a job level assigned to it. Each job posting was therefore classified according to whether it was entry-level, mid-level, senior level or executive-level. Those that did not specify the job level were classified under "Not Specified". Entry-level jobs made up the majority of the job postings (101 postings, 36.1%), followed by mid-level (87 postings, 31.1%) and senior level (65 postings, 23.2%). Executive-level only made up 3.5% of the total job postings, while 6.1% did not specify a job level.

4.4 Qualifications and Certifications

The minimum required qualifications and most common certifications listed in the job postings were analysed. Of the 280 job postings analysed, 231 job postings (82.5%) listed a specific requirement in terms of formal tertiary education. This implies a strong emphasis on meeting specific academic requirements to enter the IT industry. More than half of the job postings (65.8%, 152 job postings) specified that they require a degree in either Computer Science, Information Systems or Information Technology, as

a minimum qualification. This indicates that there is a demand for academic qualifications needed for most of the job postings and that in most cases a diploma would not suffice. A diploma was specified as a requirement for 69 job postings (29.9%), with 10 job postings (4.3%) requiring either a master's degree or some form of relevant postgraduate qualification.

In terms of certifications, Certified Information Systems Security Professional (CISSP) was the most listed (55 times in the 280 job postings). This was followed by Information Technology Infrastructure Library (ITIL) with 46 listings, and two of the certifications provided by COMPTIA, namely, Network+ with 45 listings and A+ with 42 listings.

The following section discusses the identified job roles and their related KSAs.

5 Job Roles Results and Findings

The job roles and knowledge areas identified during the thematic content analysis were mapped against the following five job categories, namely:

- Cybersecurity [CS]
- Operations and Support [OS]
- Data and Artificial Intelligence [DA]
- Strategy and Governance [SG]
- Software and Application Development [SA].

Furthermore, the skills and abilities identified during the thematic content analysis were grouped according to whether they were technical or non-technical in nature.

5.1 Identified Job Roles, Knowledge, Skills and Abilities

Table 1 presents the 20 job roles categorised according to the five job categories listed above. Cybersecurity had seven related job roles (CSJ01 to CSJ07), followed by Strategy and Governance with six (SGJ01 to SGJ06) and Data and Artificial Intelligence with three (DAJ01 to DAJ03). Operations and Support (OSJ01 and OSJ02) and Software and Application Development (SAJ01 and SAJ02) each had two related job roles identified.

Table 1. Job roles identified per job category

Code	Description	Code	Description
Cybersecurity [CS]		**Strategy and Governance [SG]**	
CSJ01	Cybersecurity Specialist	SGJ01	Information Technology Manager
CSJ02	Digital Forensics Analyst	SGJ02	Information Technology Auditor
CSJ03	Security Engineer	SGJ03	Compliance Specialist

(*continued*)

Table 1. (*continued*)

Code	Description	Code	Description
CSJ04	Data Privacy and Protection Specialist	SGJ04	Project Manager
CSJ05	Cybersecurity Manager	SGJ05	Quality Assurance Analyst
CSJ06	Application Security Specialist	SGJ06	Chief Information Officer
CSJ07	Penetration Tester	**Data and Artificial Intelligence [DA]**	
Operations and Support [OS]		DAJ01	Systems Administrator
OSJ01	Desktop Technician	DAJ02	Data Warehousing Engineer
OSJ02	Network Engineer	DAJ03	Cloud Architect
Software and Application Development [SA]			
SAJ01	Software Developer		
SAJ02	DevOps Engineer		

Table 2 presents the 54 knowledge areas identified and categorised according to their relevant job category. The most knowledge areas fall within the Strategy and Governance job category (SGK01 to SGK15), followed by Operations and Support (OSK01 to OSK13).

Table 2. Knowledge areas identified per job category

Code	Description	Code	Description	Code	Description
Cybersecurity [CS]		**Strategy and Governance [SG]**		**Software and Application Development [SA]**	
CSK01	Security Proxies	SGK01	Project Management	SAK01	SDLC
CSK02	Security Frameworks	SGK02	IT Risk	SAK02	Secure Coding
CSK03	Anti-Virus Software	SGK03	NIST	SAK03	Application Security
CSK04	Security Best Practices	SGK04	ISO	SAK04	SQL
CSK05	Penetrating Testing	SGK05	COBIT	SAK05	Coding Languages
CSK06	Security Vulnerabilities and Exploits	SGK06	Business Operations	SAK06	Functions
CSK07	Firewalls	SGK07	King IV	SAK07	Databases

(*continued*)

Table 2. (*continued*)

Code	Description	Code	Description	Code	Description
CSK08	SSL	SGK08	Problem Management	SAK08	Stored Procedures
CSK09	IPS/IDS	SGK09	Incident Management	SAK09	Database Design
Operations and Support [OS]		SGK10	Access Management	SAK10	SAK10
		SGK11	Compliance	SAK11	Version Control
OSK01	Operating Systems	SGK12	Change Management		
OSK02	PC Hardware and Software	SGK13	IT Governance		
OSK03	Backups	SGK14	ITIL		
OSK04	VMWare	SGK15	IT Security Policies		
OSK05	Active Directory	**Data and Artificial Intelligence [DA]**			
OSK06	VPN				
OSK07	IIS	DAK01	Data Warehousing		
OSK08	OWASP	DAK02	Data Analysis		
OSK09	Routers	DAK03	Data Modelling		
OSK10	Switches	DAK04	Machine Learning		
OSK11	IP/VOIP/TCP	DAK05	Cloud Services		
OSK12	Network Security	DAK06	Automation		
OSK13	Network Monitoring Tools				

Table 3 presents the 23 skills identified and categorised according to their technical or non-technical nature. 17 skills were identified as non-technical (NTS01 to NTS17) and six were considered to be technical (TS01 to TS06).

Table 3. Non-technical and technical skills identified

Code	Description	Code	Description
Non-technical skills		**Technical skills**	
NTS01	Planning Skills	TS01	Troubleshooting Skills
NTS02	Leadership Skills	TS02	Technical writing Skills
NTS03	Presentation Skills	TS03	Diagnostic Skills
NTS04	Analytical thinking Skills	TS04	General programming Skills
NTS05	Communication Skills	TS05	Administration Skills
NTS06	Adaptability Skills	TS06	Problem solving Skills
NTS07	Fast learner Skills		
NTS08	Organisational Skills		
NTS09	Time management Skills		
NTS10	Attention to detail Skills		
NTS11	Conflict management Skills		
NTS12	Collaboration Skills		
NTS13	Customer service Skills		
NTS14	Strategic thinking Skills		
NTS15	Negotiation Skills		
NTS16	Decision making Skills		
NTS17	Logical thinking Skills		

Table 4 presents the 16 non-technical abilities (NTA01 to NTA16) and 11 technical abilities (TA01 to TA11) that were identified.

Table 4. Non-technical and technical abilities identified

Code	Description	Code	Description
Non-Technical Abilities		**Technical Abilities**	
NTA01	Ability to manage human resources	TA01	Ability to solve technical problems
NTA02	Ability to lead teams	TA02	Ability to write reports
NTA03	Ability to work with leadership	TA03	Ability to obtain forensic evidence
NTA04	Ability to work in teams	TA04	Ability to provide technical assistance

(*continued*)

Table 4. (*continued*)

Code	Description	Code	Description
NTA05	Ability to maintain confidentiality	TA05	Ability to troubleshoot
NTA06	Ability to research	TA06	Ability to maintain hardware and software
NTA07	Ability to manage many priorities concurrently	TA07	Ability to analyse data
NTA08	Ability to engage and contribute	TA08	Ability to investigate malware, intrusion attempts and vulnerabilities
NTA09	Ability to execute instructions	TA09	Ability to learn new technology independently
NTA10	Ability to be proactive and efficient	TA10	Ability to create network diagrams and related documentation
NTA11	Ability to work under pressure	TA11	Ability to write secure code
NTA12	Ability to adapt to changing environments		
NTA13	Ability to stay organised		
NTA14	Ability to communicate effectively and efficiently		
NTA15	Ability to prioritise		
NTA16	Ability to work independently		

The skills depicted in Table 3 and the abilities shown in Table 4 were further analysed and mapped against the five main job categories, as discussed in the next sub-section.

5.2 Mapping of Identified Skills and Abilities to Job Categories

Table 5 highlights the four most relevant non-technical skills, namely: NTS04 (Analytical thinking skills), NTS05 (Communication skills), NTS10 (Attention to detail skills), as well as NTS17 (Logical thinking skills). NTS04, NTS05, NTS10 and NTS17 are required by all job categories. Further, both Cybersecurity [CS] and Strategy and Governance [SG] require 15 of the 17 identified non-technical skills.

Notable technical skills shown in Table 6 are TS01 (Troubleshooting skills) and TS06 (Problem solving skills). TS01 is present in all job categories identified and TS06 had been identified in all but one category, Software and Application development [SA]. Cybersecurity [CS] has been shown to require all but one of the technical skills identified.

Table 5. Non-technical skills mapped according to job categories

	Non- Technical Skills																
Job Category	NTS 01	NTS 02	NTS 03	NTS 04	NTS 05	NTS 06	NTS 07	NTS 08	NTS 09	NTS 10	NTS 11	NTS 12	NTS 13	NTS 14	NTS 15	NTS 16	NTS 17	TOTAL
CS																		15
OS																		8
DA																		8
SG																		15
SA																		9
TOTAL	2	3	2	5	5	4	3	4	3	5	2	3	1	2	2	4	5	

Table 6. Technical skills mapped according to job categories

	Technical Skills						
Job	TS01	TS02	TS03	TS04	TS05	TS06	TOTAL
CS							5
OS							4
DA							4
SG							3
SA							4
TOTAL	5	3	3	3	2	4	

It can be seen in Table 7 that TA01 (Ability to solve technical problems) and TA05 (Ability to troubleshoot) have been identified as required for all the identified job categories. Cybersecurity [CS], Operations and Support [OS] as well as Data and Artificial Intelligence [DA] mapped against 7 of the 11 technical abilities.

Table 7. Technical abilities mapped according to job categories

	Technical Abilities											
Job	TA01	TA02	TA03	TA04	TA05	TA06	TA07	TA08	TA09	TA10	TA11	TOTAL
CS												7
OS												7
DA												7
SG												5
SA												5
TOTAL	5	2	1	4	5	2	4	1	3	2	2	

As seen in Table 8, both NTA04 (Ability to work in teams) and NTA09 (Ability to execute instructions) are required by all identified job categories. Further, Cybersecurity [CS] and Strategy and Governance [SG] both required 13 of the 17 non-technical abilities identified.

The mappings of the various skills and abilities to the five job categories identified by this study provides valuable detail for companies offering positions relating to these job categories and related job roles.

Table 8. Non-technical abilities mapped according to job categories

	Non-Technical Abilities																
Job Category	NTA 01	NTA 02	NTA 03	NTA 04	NTA 05	NTA 06	NTA 07	NTA 08	NTA 09	NTA 10	NTA 11	NTA 12	NTA 13	NTA 14	NTA 15	NTA 16	TOTAL
CS																	13
OS																	7
DA																	10
SG																	13
SA																	6
TOTAL	1	3	2	5	3	3	4	3	5	3	3	4	2	4	1	3	

6 Discussion and Implications

From this study it is evident that IT professionals with cybersecurity KSAs are required in various industries in South Africa. Many job postings specified the job as an entry-level position, despite there being a need for security knowledge, and in some cases, certifications related to cybersecurity for these entry-level positions. CISSP was the most mentioned certification, yet it requires a minimum of 5 years cybersecurity experience to qualify for the certification. In 65.8% of the job postings, the employers expect the ideal candidate to have a degree in either Computer Science, Information Systems or Information Technology. In addition, cybersecurity-related certifications were considered an advantage, if not a requirement, for many of the 280 job postings analysed. It was interesting to note that there were some cases where an entry-level job required a CISSP certification, as well as a relevant degree, further indicating the high level of experience and academic requirements for IT professionals with cybersecurity KSAs. Skills and abilities relating to the Cybersecurity [CS] job category is by far the most in demand based on the job postings analysed.

Several trends were identified from this study. Table 2 presents the knowledge areas found in the 280 job postings analysed. However, many of the knowledge areas could be considered as technical skills rather than knowledge areas. For example, Penetration Testing (CSK05) and Secure Coding (SAK02) are often considered to be technical skills. However, employers seem to focus more on knowledge requirements and non-technical skills, with the technical skills mentioned being less specific and more generalised, for example Problem-Solving skills (TS06). This is also evident in Table 3, when comparing the number of technical (6) and non-technical (17) skills. It is interesting to note the emphasis on non-technical skills and abilities especially in the Cybersecurity [CS] and Strategy and Governance [SG] job categories.

Based on this study one can more clearly determine what is required in terms of KSAs when employing IT professionals in the five identified job categories. This information could be used towards a cybersecurity skills framework for South Africa, which may contribute to improving the South African cybersecurity posture.

The KSAs identified in this study closely align with the Skills Framework for Infocomm Technology (SFw for ICT), sharing many knowledge areas, skills and abilities. Due to this study's alignment with (SFw for ICT), it could provide a good baseline for a cybersecurity skills framework for South Africa. This could be used to better inform

employers and future employees, as well as to assist in the further development of cybersecurity curricula in the education sector.

7 Conclusion

Despite the limitation of only analysing job postings over a four-month period from 1st October 2020 to 31st January 2021, this study contributed further understanding of the cybersecurity skills demand in South Africa. In addition, it demonstrated that ATLAS.ti is a suitable tool to use for analysing such datasets using the three-phased approach as proposed by [15].

Most countries are developing their own workforce and skills frameworks for IT and cybersecurity professionals. Australia, Canada, the United Kingdom and Singapore are among those who have developed, or are in the process of developing, their own frameworks. South Africa has a need for a similar framework that identifies cybersecurity knowledge, skills and abilities for different IT and cybersecurity job roles in the South African context. Future work will therefore use the results of this study to propose a cybersecurity skills framework for the South African context.

References

1. CEI: Country statistics – cyber exposure index (2020). https://cyberexposureindex.com/country-statistics/
2. Smith, C.: Major spike in SA cyber attacks, over 10 000 attempts a day. News24 (2019). https://www.fin24.com/Companies/ICT/major-spike-in-sa-cyber-attacks-over-10-000-attempts-a-day-security-company-20190429
3. Cisco: What is cybersecurity? - Cisco (2017). https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html
4. Tunggal, A.T.: What is a cyber threat? Upguard (2020). https://www.upguard.com/blog/cyber-threat
5. Ahola, M.: The role of human error in successful cyber security breaches. Usecure (2019). https://blog.getusecure.com/post/the-role-of-human-error-in-successful-cyber-security-breaches
6. Parker, A., Brown, I.: Skills requirements for cyber security professionals: a content analysis of job descriptions in South Africa. In: Venter, H., Loock, M., Coetzee, M., Eloff, M., Eloff, J. (eds.) ISSA 2018. CCIS, vol. 973, pp. 176–192. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-11407-7_13
7. Oltsik, J.: 2017 ISSA ESG survey results - information systems security association (2017). https://www.members.issa.org/page/2017_issaesg_surv
8. Oltsik, J.: ESG Research report: the life and times of cybersecurity professionals 2020, July 2020. https://www.esg-global.com/research/esg-research-report-the-life-and-times-of-cybersecurity-professionals-2020
9. ISACA: ISACAs State of Cybersecurity 2019 Survey Retaining Qualified Cybersecurity Professionals (2019). https://www.isaca.org/why-isaca/about-us/newsroom/press-releases/2019/isacas-state-of-cybersecurity-2019-survey-retaining-qualified-cybersecurity-professionals
10. Burning Glass Technologies: The State of Cybersecurity Hiring, pp. 1–26, June 2019
11. Bucchianeri, S.: The cybersecurity skills gap offers SA an opportunity to lead in the 4IR (2019). https://www.iol.co.za/business-report/opinion/the-cybersecurity-skills-gap-offers-sa-an-opportunity-to-lead-in-the-4ir-31762949

12. Doyle, K.: Wanted: cyber security expertise | ITWeb. ITWeb's Corporate IT Training Guide, 4th Issue, p. 27 (2016). http://books.itweb.co.za/tg/
13. NIST: NICE Cybersecurity Workforce Framework Use Cases and Success Stories. Engl. J. 1–21 (2020). https://www.nist.gov/news-events/events/2020/03/nice-webinar-nice-cybersecurity-workforce-framework-use-cases-and-success
14. IMDA: Skills Framework For ICT (2017). https://www.imda.gov.sg/cwp/assets/imtalent/skills-framework-for-ict/index.html
15. Soratto, J., de Pires, D.E.P., Friese, S.: Thematic content analysis using ATLAS.ti software: potentialities for researchs in health. Rev. Bras. Enfermagem **73**(3), e20190250 (2020). https://doi.org/10.1590/0034-7167-2019-0250